UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

---

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124

v.

MARCUS HUTCHINS,

Defendant.

---

**DEFENDANT'S REPLY IN SUPPORT OF MOTION TO DISMISS THE INDICTMENT (FAILURE TO STATE OFFENSES) (DOC. NO. 56)**

---

The government fails to allege any acts by Marcus Hutchins which, if proven, would constitute violations of the Computer Fraud and Abuse Act or the Wiretap Act. Because there is no case to prove, the Court should dismiss all counts with prejudice against Mr. Hutchins.

**1. Counts One and Six Do Not State an Offense**

The government first argues that the indictment needs only to repeat verbatim the language of the invoked statutes to satisfy the pleading requirements of a federal criminal case. (Gov't Response at 3 (Doc. No. 65).) In this regard, the government confuses what is technically required with what is substantively necessary. Here, the government's characterization of the undisputed facts does not "constitute a violation of any statute," so there is "no

case to prove" and the indictment is properly subject to dismissal for that reason. *United States v. Risk*, 843 F.2d 1059, 1060 (7th Cir. 1988).

Next, the government suggests that its characterization of Kronos as "malware" should satisfy the pleading standard, claiming that it is "common knowledge" that malware is "written with the intent of being disruptive or damaging." (Gov't Response at 4 (citing Oxford English Dictionary 2018).) But the CFAA does not make so-called malware illegal—it is not some form of contraband. In fact, the term "malware" does not appear anywhere in the statute. The CFAA is not concerned with what software is called, but what an actor uses it to do.

Artificial labels aside, the question before the Court is whether the indictment adequately pleads a case that Mr. Hutchins and his co-defendant conspired or attempted to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer." 18 U.S.C. §§ 371 & 1030(a)(5)(A). The only definition of "malware" relevant to that question is one offered in the indictment.

The indictment, at paragraph 3(d), defines "malware" as "malicious computer code installed on protected computers without authorization that allowed unauthorized access to the protected computer." Nothing in this definition involves "intentionally caus[ing] damage without authorization, to a

protected computer," which is necessary to violate § 1030(a)(5)(A). The indictment's "unauthorized access" language seems to be borrowed from other provisions of the CFAA that have not been charged in this case, such as §§ 1030(a)(2), (5)(B), and (5)(C)—all of which include additional elements beyond "unauthorized access." Even if Kronos precisely meets the definition of "malware" offered by the government in the indictment, that functionality alone would not constitute a violation of § 1030(a)(5)(A) or any other provision of the CFAA. The government's argument here therefore misses the point and is without merit.

Finally, the government's attempt at distinguishing this case from the binding precedent of the Seventh Circuit is ineffective. The government offers *Fidlar Technologies v. LPS Real Estate Data Solutions* for the idea that "damage" as defined by the CFAA includes "clearly destructive behavior such as using a virus or worm or deleting data . . . [as well as] less obvious invasive conduct, such as flooding an email account." 810 F.3d 1075, 1084 (7th Cir. 2016). Yet the government does not argue that Kronos is a virus or worm, or that it deletes data, or that it floods email accounts. The indictment alleges only that Kronos copies data and exfiltrates it. This functionality is more like "simply download[ing] data without leaving a trace," which the court in *Fidlar Technologies* determined was *not* damage. *Id*. at 1084.

**2. Counts Two Through Five Do Not State an Offense**

In arguing that Kronos is a "electronic, mechanical, or other device" for purposes of 18 U.S.C. § 2511 and 2512, the government steers the Court's attention to legal issues that are not relevant to the issues raised by Mr. Hutchins' motion. As such, the government's arguments should be rejected.

The government notes that *Potter v. Havicek*—the case that most directly examines the issue of whether software alone can be a wiretapping device—deals with manufacturer liability for civil damages under § 2520, which creates a private right of action. (Gov't Response at 7-8.) But since this is a criminal case, that aspect of *Potter* is irrelevant. What *is* relevant to this criminal case is *Potter's* conclusion that the software in that case was not an "electronic, mechanical, or other device" as defined by the Wiretap Act. 2008 WL 2556723, at **8-9 (S.D. Ohio June 23, 2008). The government neglects to address this, a circumstance that does not turn on distinctions between civil and criminal liability.

The government next contends that *United States v. Szymuszkiewicz,* 622 F.3d 701, 707 (7th Cir. 2010) (as amended Nov. 29, 2010), "does not address the issue in this case" and claims that the defense misstates the case's "holding." (Gov't Response at 8.) A holding "involves a determination of a matter of law that is pivotal to a judicial decision." Bryan A. Garner, *Garner's Dictionary of Legal Usage* 412 (3d ed. 2011). Courts can—and often do—make more than one holding in a case.

The government is correct that *Szymuszkiewicz* held that a device used to intercept a communication may be the same as the device used to receive that communication. 622 F.3d at 707. But the court there *also* held that the defendant acquired communications using computers. *Id.* The computers were the relevant devices for purposes of the offense. *Id.* Software was not.

The government also relies on several cases that considered whether software installed on computers "intercepted" communications within the meaning of the Wiretap Act, or accessed stored communications within the meaning of a different statute, the Stored Communications Act. (Gov't Response at 6-8, citing to *Luis v. Zeng,* 2013 WL 811816, at **3-7 (S.D. Ohio March 5, 2013), *recommendation adopted, reversed on other grounds by* 833 F.3d 619 (6th Cir. 2016); *Shefts v. Petrakis,* No. 10-cv-1104, 2012 WL 4049484, at *9 (C.D. Ill. Sept. 13, 2012); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661 (E.D. Tenn. July 19, 2012).) But because none of the defendants in those cases raised the issue, none of the cases addressed the question of whether the software or the computer was the relevant "device" for purposes of the Wiretap Act.

That makes sense: those cases all involved claims that the defendants acquired communications using software running on a computer. Under those circumstances, a court has no reason to draw a distinction between the two because the software and computer are working together: the operation of one depends on the other. Indeed, the cases cited by the government discuss

computers and the software installed on them as one unit. *See, e.g.*, *Zang*, 833 F.3d at 633 ("[O]nce installed on a computer, WebWatcher automatically acquires and transmits communications to servers"); *Klumb*, 884 F. Supp. 2d at 661 ("The point is that a program has been installed on the computer which will cause emails sent at some time in the future through the internet to be re-routed[.]"); *see also Shefts,* 2012 WL 4049484, **6-10 (variously referring to servers, email accounts, software, and BlackBerry smartphones as interception devices).

For purposes of the § 2512 charges in this case, however, the distinction between software and computer is important. In Counts Two through Four, there *is* no computer, which would not be true in any scenario involving an actual interception. As noted in *Potter*, software alone is incapable of intercepting anything. 2008 WL 2556723, at *8. "It must be installed in a device, such as a computer, to be able to do so." *Id*.

The government also cites *United States v. Barrington* to support its position that keylogger software is a "electronic, mechanical, or other device" under the Wiretap Act. 648 F.3d 1178, 1201 (11th 2011). *Barrington*, however, says no such thing. *Barrington* considered whether a keylogger was "device-making equipment" or a "scanning receiver" under 18 U.S.C. § 1029, a statute that prohibits fraud and related activity in connection with access devices. *Id.* at 1201-02. That statute is not at issue in this case. In fact, the court in *Barrington* concluded there was *no* evidence that the keylogger was "a device or apparatus

that can be used to intercept a wire or electronic communication in violation of [the Wiretap Act]." *Id*. at 1203.

The government also claims that Counts Two and Five do not depend on Kronos alone qualifying as a "device." (Gov't Response at 8-9.) First, the government argues that Count Two should survive because the defendants allegedly used a YouTube video to demonstrate Kronos operating on a computer and posted descriptions of how it operates on a computer in hacking forums. (Gov't Response at 8-9.) As an initial matter, the government is directing the Court to facts outside the four corners of the indictment, which Federal Rule of Criminal Procedure 12(d) does not permit on a motion to dismiss. *United States v. Bryant*, 2013 WL 3423275, at **5-6 (E.D. Wis. July 8, 2013) (Joseph, M.J.). Furthermore, the indictment does not contain any reference to YouTube or allege that either defendant posted descriptions of how Kronos operates on a computer. It alleges that "a video showing the functionality" of Kronos "was posted to a publicly available website"—and, importantly, does not attribute the posting to the defendants. (Indictment ¶ 4(b).) The indictment also alleges that Mr. Hutchins' co-defendant "used the video to demonstrate how Kronos worked," and that the co-defendant "offered to sell" and "advertised the availability" of Kronos on internet forums. (*Id.*¶ 4(c) & (e).) The indictment does not claim that the defendants advertised Kronos operating on a computer for sale.

And § 2512(1)(c)(1) does not make it illegal to demonstrate or describe how a device functions; it makes it illegal to advertise certain devices for sale.

Turning to Count Five, the government argues that even if Kronos does not qualify as a "device," the defendants transmitted it to another person knowing and intending that that individual would use it to intercept communications. (Gov't Response at 9.) This argument fails because the indictment does not support the conclusion that the defendants transmitted Kronos to another person knowing and intending that that individual would use it to intercept communications. The indictment does not allege that the defendants intended the buyer to do anything in particular, as discussed in more detail below.

Next, the government offers an array of dictionary definitions to argue that the common meanings of "device," "mechanism," and "apparatus" are more expansive than the dictionary definition of "device" offered by the defense. (Gov't Response at 8-10.) None of the government's suggested definitions says anything about software or provides reason to conclude that software-in-isolation is an "electronic, mechanical, or other device." The defense has offered the Merriam-Webster dictionary definition that the court in *Potter* found to be the most germane for interpreting the Wiretap Act. 2008 WL 2556723, at *8. That court did not consider the more all-encompassing definitions (like those offered by the government) to be persuasive. *Id.*

Finally, the government urges the Court to interpret "electronic, mechanical, or other device" broadly to accommodate new developments in technology since the Wiretap Act was passed in 1968. (Gov't Response at 10-11.) But when Congress wishes to make something illegal, it knows how to do so—it passes a new law or amends an existing one. And even though Congress has amended the Wiretap Act six times, it has never seen fit to expand the definition of "electronic, mechanical, or other device" to include software. In fact, Congress has been careful to limit the reach of §§ 2511 and 2512, increasing the level of mens rea in both statutes from "willful" to "intentional." Electronic Communications Privacy Act, Pub. L. 99-508, Title I, § 101(f), 100 Stat. 1853 (1986).

**3. Counts One, Five, and Six Fail to Allege the Requisite Intent**

The government contends that Mr. Hutchins' challenge to Counts One, Five, and Six for their failure to allege the necessary intent and causation should be rejected because it actually challenges the sufficiency of the evidence anticipated at trial and attempts to apply civil pleading standards to a criminal indictment. (Gov't Response at 12-13.) The government's argument is predictable, and wrong. *See United States v. Risk,* 843 F.2d 1059, 1060 (7th Cir. 1988) (when "the government's characterization of the undisputed facts [does] not constitute a violation of any [federal] statute," dismissal of a case before trial is appropriate under Rule 12(b)(1)).

The defense does not does not challenge the sufficiency of the evidence anticipated at trial, but the allegations in the indictment. The indictment must state "the essential facts of the crimes charged." Fed. R. Crim. P. 7(c)(1). That standard is not watered down, as the government suggests, for inchoate offenses such as conspiracy and attempt.

To engage in a conspiracy to violate a particular statute, a conspirator "must intend to further an endeavor which, if completed, would satisfy *all of the elements* of a substantive criminal offense[.]" *Salinas v. United States*, 522 U.S. 52, 65 (1997) (emphasis added). Attempts are no different—they require an intent to carry out acts that satisfy each element of the relevant crime. *United States v. Morris*, 827 F.3d 696, 699 (7th Cir. 2016) (Hamilton, J., concurring).

To violate § 1030(a)(5)(A), one must *intentionally* cause damage to a protected computer. By extension, conspiring to violate that statute requires the intent to further an endeavor which, if completed, would intentionally cause damage to a protected computer. And attempting a violation of that statute requires the intent to intentionally cause damage to a protected computer. But the indictment does not allege that Mr. Hutchins or his co-defendant intended the sale of Kronos to produce any particular outcome, much less that they intended to damage a protected computer.

Count Five has a similar flaw. That count alleges that the defendants "knowingly and intentionally endeavored to intercept and procure any other

person to intercept certain electronic communications[.]" The indictment does not reflect that Mr. Hutchins or his co-defendant intended the sale of Kronos to have any specific result, much less that either knew and intended for the buyer to use Kronos to intercept certain electronic communications.

***

The indictment's infirmities are fatal to the government's ability to move forward with this prosecution. Mr. Hutchins therefore respectfully asks that the indictment be dismissed with prejudice.

DATED: April 30, 2018

Respectfully submitted,

*/s/ Marcia Hofmann*
MARCIA HOFMANN
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Email: marcia@zeitgeist.law
Telephone: (415) 830-6664

*/s/ Brian E. Klein*
BRIAN E. KLEIN
Baker Marquart LLP
2029 Century Park E – Suite 1600
Los Angeles, CA 90067
Email: bklein@bakermarquart.com
Telephone: (424) 652-7800

*/s/ Daniel W. Stiller*
DANIEL W. STILLER
DStillerLLC

Box 511130
Milwaukee, WI 53203
Email: dan@dstillerllc.com
Telephone: (414) 207-3190

*Attorneys for Marcus Hutchins*